

Multiplicative quadratic maps

Matthias Grüninger*

Université catholique de Louvain
 Institute pour recherche en mathématique et physique
 Chemin du Cyclotron 10, bte. L7.01.01.
 1348 Louvain-la-Neuve
 Belgique

July 29, 2014

Abstract

In this paper we prove that a multiplicative quadratic map between a unital ring K and a field L is induced by a homomorphism from K into L or a composition algebra over L . Especially we show that if K is a field, then every multiplicative quadratic map is the product of two field homomorphisms. Moreover, we prove a multiplicative version of Artin's Theorem showing that a product of field homomorphisms is unique up to multiplicity.

27.07.2014 This work was completed with the support by the ERC (grant # 278 469)

1 Introduction

We begin with the following definition:

Definition 1.1 *Let K and L be (not necessarily associative) rings with 1. A map $q : K \rightarrow L$ is called a multiplicative quadratic map if*

- (a) $q(ab) = q(a)q(b)$ for all $a, b \in K$.
- (b) $q(n \cdot 1_K) = n^2 \cdot 1_L$ for all $n \in \mathbb{Z}$.
- (c) *The map $f : K \times K \rightarrow L$ defined by $f(a, b) = q(a + b) - q(a) - q(b)$ is biadditive.*

If M is a composition algebra over L with norm N and $\varphi : K \rightarrow M$ a non-zero homomorphism, then $q : K \rightarrow L : a \mapsto N(a^\varphi)$ is a multiplicative quadratic map. If $\text{char} L = 2$, then every non-zero homomorphism from K to L is a multiplicative quadratic map. We will show that if L is a field, then these are in fact all multiplicative quadratic maps between K and L .

*supported by the ERC (grant # 278 469)

Theorem 1.2 *Let K be a unital ring with 1 and L a field. If $q : K \rightarrow L$ is a multiplicative quadratic map, then one of the following holds:*

- (a) *There is a composition algebra M over L and a homomorphism $\varphi : K \rightarrow M$ with $q(a) = N(a^\varphi)$ for all $a \in K$, where N is the norm of M .*
- (b) *$\text{char} L = 2$ and q is a ring homomorphism.*

For arbitrary rings the situation is more complicated, especially in even characteristic. For example, let $K = \mathbb{Z}/2\mathbb{Z}$ and $L = \mathbb{Z}/4\mathbb{Z}$. Then the map $q : K \rightarrow L$ defined by $q(1) = 1$ and $q(0) = 0$ is a multiplicative quadratic map. Another example for a multiplicative quadratic map is the adjoint map $\# : K \rightarrow K^{op}$ with K a cubic algebra and K^{op} its opposite algebra.

We are mainly interested in the case that K is a field as well. Here we get

Corollary 1.3 *If K and L are fields, \bar{L} the algebraic closure of L and $q : K \rightarrow L$ is a multiplicative quadratic map, then there are monomorphisms $\varphi_1, \varphi_2 : K \rightarrow \bar{L}$ with $q(a) = a^{\varphi_1} a^{\varphi_2}$.*

The uniqueness of φ_1 and φ_2 in 1.3 can be easily deduced from Artin's Theorem. Our second main theorem, which can be seen as a multiplicative version of Artin's Theorem, is a generalization of this fact.

Theorem 1.4 *Let K, L be fields, $n \geq m \geq 1$ natural numbers and $\sigma_1, \dots, \sigma_n, \tau_1, \dots, \tau_m : K \rightarrow L$ field homomorphisms. Suppose that $\prod_{i=1}^n a^{\sigma_i} = \prod_{j=1}^m a^{\tau_j}$ for all $a \in K$. Then one of the following holds:*

- (a) *$n = m$ and there is a permutation $g \in S_n$ with $\tau_i = \sigma_{ig}$ for $1 \leq i \leq n$.*
- (b) *$\text{char} K = \text{char} L = p > 0$ and there are $1 \leq i_1 < i_2 < \dots < i_p \leq n$ with $\sigma_{i_1} = \sigma_{i_2} = \dots = \sigma_{i_p}$. Moreover, for all $1 \leq j \leq m$ there is an integer l with $-(m-1) \leq l(p-1) \leq n-1$ and a natural number $1 \leq i \leq n$ with $\tau_j = \sigma_i \mathbf{p}^l$ and for all $1 \leq i \leq n$ there is an integer l with $-(n-1) \leq l(p-1) \leq m-1$ and $1 \leq j \leq m$ with $\sigma_i = \tau_j \mathbf{p}^l$. Here \mathbf{p} denotes the Frobenius endomorphism of L .*

For $n = m = 2$ we get $\{\sigma_1, \sigma_2\} = \{\tau_1, \tau_2\}$ or $\text{char} K = \text{char} L = 2$ and $\sigma_1 = \sigma_2$ and $\tau_1 = \tau_2$. Hence $\sigma_1 \mathbf{p} = \tau_1 \mathbf{p}$ and so $\sigma_1 = \tau_1$.

As another corollary we get

Corollary 1.5 *Let K be a field and S a set of field endomorphisms of K . Suppose that $\text{char} K = 0$ or $\text{char} K = p$ and that if $\sigma, \tau \in S$ and $n \in \mathbb{N}$ with $\sigma = \mathbf{p}^n \tau$, then $\sigma = \tau$. Then S is \mathbb{Z} -linear independent in $\text{End}(K^*)$.*

The initial motivation for these questions lays in the theory of Moufang sets and its connection to (twin) trees. (See [2] for an introduction into this topic.) Suppose that T is a tree and G a subgroup of $\text{Aut} T$ such that the following hold:

- (a) For every vertex x of T there is a field K_x such that G_x induces a group isomorphic to $PSL_2(K_x)$ on the neighbourhood of x .

- (b) G induces a Moufang set on the set of ends of T , i.e. for every end e the group G_e has a normal subgroup U_e which acts regularly on the set of ends distinct from e .

Then under certain conditions we get multiplicative quadratic maps between K_x and K_y for all vertices x and y . The classification of all multiplicative quadratic maps helps us to classify these trees. We refer to two forthcoming papers ([3],[4]) which will use both of our main theorems.

2 Multiplicative quadratic maps

In the following K and L are rings and $q : K \rightarrow L$ is a multiplicative quadratic map with associated biadditive map f .

Lemma 2.1 *Let $a, b, c, d \in K$. Then*

- (a) $f(ac, bc) = f(a, b)q(c)$ and $f(ca, cb) = q(c)f(a, b)$.
- (b) $f(a, b)f(c, d) = f(ac, bd) + f(ad, bc)$.
- (c) *If I is a right ideal of K , then $I^\perp := \{a \in K; f(a, b) = 0 \ \forall b \in I\}$ is also a right ideal of K . The same holds for left ideals of K .*
- (d) $\text{rad}(q) := \{a \in K^\perp; q(a) = 0\}$ is an ideal of K .
- (e) $\bar{q} : K/\text{rad}(q) \rightarrow L : a + \text{rad}(q) \mapsto q(a)$ is a well-defined multiplicative quadratic map with $\text{rad}(\bar{q}) = 0$.

Proof.

- (a) We have

$$f(ac, bc) = q(ac+bc) - q(ac) - q(bc) = (q(a+b) - q(a) - q(b))q(c) = f(a, b)q(c).$$

The second equation follows by a similar computation.

- (b) By 1. we have

$$\begin{aligned} q(a+b)q(c+d) &= (q(a) + q(b) + f(a, b))(q(c) + q(d) + f(c, d)) = \\ &= q(ac) + q(ad) + f(ac, ad) + q(bc) + q(bd) + f(bc, bd) + f(ac, bc) \\ &\quad + f(ad, bd) + f(a, b)f(c, d). \end{aligned}$$

On the other hand,

$$\begin{aligned} q(a+b)q(c+d) &= q(ac+ad+bc+bd) = \\ &= q(ac) + q(ad) + q(bc) + q(bd) + f(ac, ad) + f(ac, bc) + f(ac, bd) \\ &\quad + f(ad, bc) + f(ad, bd) + f(bc, bd). \end{aligned}$$

If we compare these two equations, we get

$$f(a, b)f(c, d) = f(ac, bd) + f(ad, bc).$$

- (c) Suppose that I is a right ideal of K , $b \in I$ and $a \in I^\perp$. If we set $d = 1$ in 2. we get

$$0 = f(a, b)f(c, 1) = f(ac, b) + f(a, bc) = f(ac, b).$$

This shows that $ac \in I^\perp$. Since f is biadditive, I^\perp is additively closed. Thus I^\perp is a right ideal of K . For left ideals of K the proof is similar.

- (d) Let $a, b \in \text{rad}(q)$ and $c, d \in K$. Then $f(a + b, c) = f(a, c) + f(b, c) = 0$ and $q(a + b) = q(a) + q(b) + f(a, b) = 0$, thus $a + b \in \text{rad}(q)$. Moreover, $a \in K^\perp$, which is an ideal of K , so also $ac \in K^\perp$ and thus $f(ac, d) = 0$. Since $q(ac) = q(a)q(c) = 0$, we get $ac \in \text{rad}(q)$.
- (e) For all $a \in K$ and $b \in \text{rad}(q)$ we get $q(a + b) = q(a) + q(b) + f(a, b) = q(a)$, so \bar{q} is well-defined. The rest is clear.

□

We will say that q is *non-degenerate* if $\text{rad}(q) = \{0\}$.

Lemma 2.2 *Suppose that $a \in K$ with $f(a, b) = 0$ for all $b \in K$. Then*

- (a) $q(a)f(b, c) = f(b, c)q(a) = 0$ for all $b, c \in K$.
- (b) *If $q(a)$ is not a zero-divisor, then $\text{char} L = 2$ and q is a ring homomorphism.*

Proof. By assumption $a \in K^\perp$, which is an ideal by 2.1. Thus for all $b, c \in K$ we have $ab, ac, ba, ca \in K^\perp$ and so $0 = f(ab, ac) = q(a)f(b, c)$ and $0 = f(ba, ca) = f(b, c)q(a)$. Thus 1. follows. If $q(a)$ is not a zero-divisor, then f is identically zero, thus q is a ring homomorphism. Since $4 \cdot 1_L = q(2 \cdot 1_K) = 2 \cdot 1_L$ holds in L , we get $\text{char} L = 2$. □

If F is a commutative, associative ring such that K and L are F -algebras, we say that q is F -quadratic if f is F -bilinear and $q(\lambda a) = \lambda^2 q(a)$ for all $a \in K$ and $\lambda \in F$. Note that q is always \mathbb{Z} -quadratic. If K and L are fields, then they have the same characteristic (since $q(n \cdot 1_K) = n^2 \cdot 1_L$ for all $n \in \mathbb{N}$), and one can easily see that q is F -quadratic with $F = \mathbb{Q}$ or $F = \mathbb{F}_p$ for a prime p .

From now on L is associative and commutative. Suppose that F is a subring of L such that K is a F -algebra and q is F -quadratic. Moreover, suppose that every finitely generated submodule of K is a free F -module. Set $\tilde{K} = L \otimes_F K$. Then \tilde{K} is a L -module. For $a \in K$ and $\lambda \in L$ we write λa instead of $\lambda \otimes a$. We define $\tilde{q} : \tilde{K} \rightarrow L$ by

$$\tilde{q}\left(\sum_{i=1}^n \lambda_i a_i\right) = \sum_{i=1}^n \lambda_i^2 q(a_i) + \sum_{1 \leq i < j \leq n} \lambda_i \lambda_j f(a_i, a_j)$$

for $a_1, \dots, a_n \in K$ and $\lambda_1, \dots, \lambda_n \in L$ and set $\tilde{f}(a, b) = \tilde{q}(a + b) - \tilde{q}(a) - \tilde{q}(b)$ for $a, b \in \tilde{K}$. Then

Proposition 2.3 *\tilde{q} is a multiplicative L -quadratic map.*

Proof. Since every finitely generated F -module of K is free, one can prove by a standard argument that \tilde{q} is well-defined. Let $a_1, \dots, a_n \in K, \lambda_1, \dots, \lambda_n, \mu_1, \dots, \mu_n \in L$ and $x = \sum_{i=1}^n \lambda_i a_i, y = \sum_{j=1}^n \mu_j a_j \in \tilde{K}$. Then

$$\begin{aligned} \tilde{f}(x, y) &= \tilde{q}\left(\sum_{i=1}^n (\lambda_i + \mu_i) a_i\right) - \tilde{q}\left(\sum_{i=1}^n \lambda_i a_i\right) - \tilde{q}\left(\sum_{i=1}^n \mu_i a_i\right) = \\ &= \sum_{i=1}^n (\lambda_i + \mu_i)^2 q(a_i) + \sum_{i < j} (\lambda_i + \mu_i)(\lambda_j + \mu_j) f(a_i, a_j) - \\ &= \sum_{i=1}^n \lambda_i^2 q(a_i) - \sum_{i < j} \lambda_i \lambda_j f(a_i, a_j) - \sum_{i=1}^n \mu_i^2 q(a_i) - \sum_{i < j} \mu_i \mu_j f(a_i, a_j) = \\ &= \sum_{i=1}^n 2\lambda_i \mu_i q(a_i) + \sum_{i < j} (\lambda_i \mu_j + \mu_i \lambda_j) f(a_i, a_j) = \\ &= \sum_{i=1}^n \lambda_i \mu_i f(a_i, a_i) + \sum_{i < j} (\lambda_i \mu_j + \lambda_j \mu_i) f(a_i, a_j) = \sum_{i, j=1}^n \lambda_i \mu_j f(a_i, a_j). \end{aligned}$$

Thus \tilde{f} is L -bilinear. By definition $\tilde{q}(\lambda a) = \lambda^2 \tilde{q}(a)$ for all $a \in \tilde{K}$ and all $\lambda \in L$. It remains to show that \tilde{q} is multiplicative. We define an ordering \subset on $\{1, \dots, n\} \times \{1, \dots, n\}$ by $(i, j) \subset (k, l)$ iff $i < k$ or $i = k$ and $j < l$. Using 2.1 we get

$$\begin{aligned} \tilde{q}(x)\tilde{q}(y) &= \left(\sum_{i=1}^n \lambda_i^2 q(a_i) + \sum_{i < k} \lambda_i \lambda_k f(a_i, a_k)\right) \left(\sum_{j=1}^n \mu_j^2 q(a_j) + \sum_{j < l} \mu_j \mu_l f(a_j, a_l)\right) = \\ &= \sum_{i, j=1}^n \lambda_i^2 \mu_j^2 q(a_i) q(a_j) + \sum_{i=1}^n \sum_{j < l} \lambda_i^2 \mu_j \mu_l q(a_i) f(a_j, a_l) + \\ &= \sum_{i < k} \sum_{j=1}^n \lambda_i \lambda_k \mu_j^2 f(a_i, a_k) q(a_j) + \sum_{i < k} \sum_{j < l} \lambda_i \lambda_k \mu_j \mu_l f(a_i, a_k) f(a_j, a_l) = \\ &= \sum_{i, j=1}^n \lambda_i^2 \mu_j^2 q(a_i a_j) + \sum_{i=1}^n \sum_{j < l} \lambda_i^2 \mu_j \mu_l f(a_i a_j, a_i a_l) + \sum_{i < k} \sum_{j=1}^n \lambda_i \lambda_k \mu_j^2 f(a_i a_j, a_k a_j) \\ &+ \sum_{i < k} \sum_{j < l} \lambda_i \lambda_k \mu_j \mu_l (f(a_i a_j, a_k a_l) + f(a_i a_l, a_k a_j)) = \\ &= \sum_{i, j=1}^n \lambda_i^2 \mu_j^2 q(a_i a_j) + \sum_{i=1}^n \sum_{j < l} \lambda_i^2 \mu_j \mu_l f(a_i a_j, a_i a_l) + \sum_{i < k} \sum_{j=1}^n \lambda_i \lambda_k \mu_j^2 f(a_i a_j, a_k a_j) + \\ &= \sum_{i < k} \sum_{j \neq l} \lambda_i \lambda_k \mu_j \mu_l f(a_i a_j, a_k a_l) = \sum_{i, j=1}^n \lambda_i^2 \mu_j^2 q(a_i a_j) + \end{aligned}$$

$$\sum_{(i,j) \subset (k,l)} \lambda_i \lambda_k \mu_j \mu_l f(a_i a_j, a_k a_l).$$

But we have

$$xy = \sum_{i,j=1}^n \lambda_i \mu_j a_i a_j$$

and thus

$$\tilde{q}(xy) = \sum_{i,j=1}^n \lambda_i^2 \mu_j^2 q(a_i a_j) + \sum_{(i,j) \subset (k,l)} \lambda_i \mu_j \lambda_k \mu_l f(a_i a_j, a_k a_l) = \tilde{q}(x) \tilde{q}(y).$$

□

Proof of Theorem 1.2. By 2.1.5. we may assume that q is non-degenerate. If $\text{char} L = p > 0$, then $q(p \cdot 1_K) = p^2 \cdot 1_L = 0$ and $f(p \cdot 1_K, a) = pf(1_K, a) = 0$ for all $a \in K$, so $\text{char} K = p$ as well. If $\text{char} L = 0$, then $q(n \cdot 1_K) = n^2 \cdot 1_L \neq 0$ for all natural numbers $n \geq 0$, so $\text{char} K = 0$ as well. So K and L have the same characteristic. Set $F = \mathbb{Z}$ if $\text{char} K = \text{char} L = 0$ and $F = \mathbb{F}_p$ if $\text{char} K = \text{char} L = p$. Using 2.3, we get a multiplicative L -quadratic map $\tilde{q} : L \otimes_F K \rightarrow L$. Thus \tilde{q} is a quadratic form of the L -vectorspace $L \otimes_F K$. Set $M := L \otimes_F K / \text{rad}(\tilde{q})$ and let $N : M \rightarrow L : N(a + \text{rad}(\tilde{q})) = \tilde{q}(a)$. Then by 2.1.5. N is well-defined. Since $\text{rad}(N) = 0$, by 2.2.2. either $\text{char} L = 2$ and N is a ring homomorphism or the bilinear form associated to N is non-degenerate. In the first case q is a homomorphism as well. Since f is identically zero and $\text{rad}(q) = \{0\}$, q must be injective.

In the second case M is a composition algebra over L with norm N . Set $\varphi : K \rightarrow M : x \mapsto 1 \otimes x + \text{rad}(N)$. Since $\text{rad}(q) = 0$, φ is an embedding of K in M with $N(x^\varphi) = q(x)$ for all $x \in K$. □

Proof of Corollary 1.3. If K is a field, then in the first case of 1.2 M must be a commutative composition algebra. Thus by 1.6.2 of [5] we have either $M = L$ and $N(x) = x^2$ for $x \in M$ or $M \cong L \times L$ and $N(x_1, x_2) = x_1 x_2$ for $(x_1, x_2) \in M$ or M is a separable quadratic extension of L and $N(x) = x x^\sigma$ for $x \in M$ with σ the non-trivial Galois automorphism of M . In the first case we have $q(x) = (x^\varphi)^2$ for an embedding $\varphi : K \rightarrow L$, in the second case there are embeddings $\varphi_1, \varphi_2 : K \rightarrow L$ with $q(x) = x^{\varphi_1} x^{\varphi_2}$, in the last case there is an embedding $\varphi : K \rightarrow M$ with $q(x) = x^\varphi x^{\varphi\sigma}$ for $x \in K$. In the second case of 1.2 we have $q(a) = a^\varphi a^\varphi$ with \overline{L} the algebraic closure of L and $\varphi : K \rightarrow \overline{L} : a \mapsto \sqrt{q(a)}$. □

3 The uniqueness of products of field homomorphisms

We will now deal with the uniqueness of the representations of maps of the form

$$x \mapsto \prod_{i=1}^n x^{\sigma_i}$$

with $\sigma_1, \dots, \sigma_n : K \rightarrow L$ field homomorphisms. In general, such a representation is not unique. For example, let $L = K$ be a field of characteristic 2, let \mathbf{p} be the Frobenius endomorphism and set $\sigma_1 = \sigma_2 = \sigma_3 := \mathbf{p}$, $\tau_1 = \mathbf{p}^2$ and $\tau_2 = \tau_3 = id$. Then we have $\prod_{i=1}^3 x^{\sigma_i} = x^6 = \prod_{i=1}^3 x^{\tau_i}$.

Lemma 3.1 *Suppose that K and L are fields and $\sigma_1, \dots, \sigma_n : K \rightarrow L$ are monomorphisms. If $\sum_{g \in S_n} \prod_{i=1}^n x_i^{\sigma_{ig}} = 0$ for all $x_1, \dots, x_n \in K$, then $\text{char} K = p > 0$ and there are $1 \leq i_1 < \dots < i_p \leq n$ with $\sigma_{i_1} = \dots = \sigma_{i_p}$.*

Proof. We have

$$\sum_{g \in S_n} \prod_{i=1}^n x_i^{\sigma_{ig}} = \sum_{i=1}^n \left(\sum_{g \in S_n, ng=i} \prod_{j=1}^{n-1} x_j^{\sigma_{jg}} \right) x_n^{\sigma_i}.$$

Set $a_i(x_1, \dots, x_{n-1}) := \sum_{g \in S_n, ng=i} \prod_{j=1}^{n-1} x_j^{\sigma_{jg}}$. Then

$$\sum_{g \in S_n} \prod_{i=1}^n x_i^{\sigma_{ig}} = \sum_{i=1}^n a_i(x_1, \dots, x_{n-1}) x_n^{\sigma_i}.$$

If $a_n(x_1, \dots, x_{n-1}) = 0$ for all $x_1, \dots, x_{n-1} \in K$, then the claim follows by induction. Suppose that there are x_1, \dots, x_{n-1} such that $a_n(x_1, \dots, x_{n-1}) \neq 0$. We may assume that there is $0 \leq m < n$ with $\sigma_i \neq \sigma_n$ for $i \leq m$ and $\sigma_i = \sigma_n$ for $i > m$. Then

$$\begin{aligned} 0 &= \sum_{g \in S_n} \prod_{i=1}^n x_i^{\sigma_{ig}} = \sum_{i=1}^m a_i(x_1, \dots, x_{n-1}) x_n^{\sigma_i} + \\ &\quad (n-m) a_n(x_1, \dots, x_{n-1}) x_n^{\sigma_n}. \end{aligned}$$

By the Theorem of Artin ([1], III 1, Satz 13) this implies

$$(n-m) a_n(x_1, \dots, x_{n-1}) = 0,$$

thus $\text{char} K = p > 0$ and p divides $n-m$. □

Proof of Theorem 1.4. We prove the claim by induction on $n+m$. For $x_1, \dots, x_n \in K$, $\emptyset \neq J \subseteq \{1, \dots, n\}$ set $x_J = \sum_{i \in J} x_i$ and

$$f(x_1, \dots, x_n) := \sum_{\emptyset \neq J \subseteq \{1, \dots, n\}} (-1)^{|J|} \prod_{i=1}^n x_J^{\sigma_i} = \sum_{\emptyset \neq J \subseteq \{1, \dots, n\}} (-1)^{|J|} \prod_{i=1}^m x_J^{\tau_i}.$$

Then

$$f(x_1, \dots, x_n) = \sum_{g \in S_n} \prod_{i=1}^n x_i^{\sigma_{ig}} = \sum_{g \in S_n} \prod_{i=1}^n x_i^{\tau_{ig}}$$

if $m = n$ and

$$f(x_1, \dots, x_n) = \sum_{g \in S_n} \prod_{i=1}^n x_i^{\sigma_{ig}} = 0$$

if $m < n$. Again, set $a_i(x_1, \dots, x_{n-1}) = \sum_{g \in S_n, ng=i} \prod_{j=1}^{n-1} x_j^{\sigma_{ig}}$. If $m = n$, we set $b_i(x_1, \dots, x_{n-1}) = \sum_{g \in S_n, ng=i} \prod_{j=1}^{n-1} x_j^{\tau_{ig}}$. If $m < n$, we set $b_i(x_1, \dots, x_{n-1}) = 0$. In both cases we have

$$\sum_{i=1}^n a_i(x_1, \dots, x_{n-1}) x_n^{\sigma_i} = f(x_1, \dots, x_n) = \sum_{i=1}^m b_i(x_1, \dots, x_{n-1}) x_n^{\tau_i}.$$

First suppose $\text{char} K = 0$ or $\text{char} K = p$ and there are no p identical σ_i , then by 3.1 there are x_1, \dots, x_n such that $f(x_1, \dots, x_n) \neq 0$. Again by Artin ([1], III 1, Satz 13) we get $m = n$ and there are i, j with $\sigma_i = \tau_j$. We may assume $i = j = n$. Then we have $\prod_{i=1}^{n-1} x_i^{\sigma_i} = \prod_{i=1}^{n-1} x_i^{\tau_i}$ for all $x \in K$ and thus 1. holds by induction.

Now suppose that $\text{char} K = \text{char} L = p$ and that $\sigma_n = \sigma_{n-1} = \dots = \sigma_{n-p+1}$. Then we have

$$a^{\sigma_1} \dots a^{\sigma_{n-p}} a^{\sigma_n \mathbf{p}} = a^{\tau_1} \dots a^{\tau_m}$$

for all $a \in K$ with \mathbf{p} the Frobenius endomorphism. Hence for all $1 \leq j \leq m$ there is a $l \in \mathbb{Z}$ with $-m+1 \leq l(p-1) \leq n-p$ such that there is an $1 \leq i \leq n-p$ with $\tau_j = \sigma_i \mathbf{p}^l$ or $\tau_j = \sigma_n \mathbf{p}^{l+1}$. In the last case we replace l by $l+1$ and get that there is an integer l with $-m+1 \leq l(p-1) \leq n-1$ and $1 \leq i \leq n$ with $\tau_j = \sigma_i \mathbf{p}^l$.

We have to prove that for $1 \leq i \leq n$ there is an integer l with $-n+1 \leq l(p-1) \leq m-1$ and $1 \leq j \leq m$ with $\sigma_i = \tau_j \mathbf{p}^l$. This follows directly for $i \leq n-p$. Moreover there is an integer l with $-n+p \leq l(p-1) \leq m-1$ and $1 \leq j \leq m$ with $\sigma_n \mathbf{p} = \tau_j \mathbf{p}^l$ and hence $\sigma_n = \tau_j \mathbf{p}^{l-1}$. If we replace l by $l-1$, the claim follows.

□

References

- [1] E. Artin, *Algebra II*, Ausarbeitung der im WS 1961/62 an der Universität Hamburg gehaltenen Vorlesung
- [2] P.-E. Caprace, T. De Medts, *Trees, contraction groups and Moufang sets*, Duke Math. J. **162** Nr. 13 (2013), pp. 2413-2449
- [3] P.-E. Caprace, M. Grüniger, *Boundary Moufang trees with abelian root groups of characteristic p* , preprint (arXiv: 1406.5940).

- [4] M. Grüninger, *Moufang twin trees whose set of ends form a Moufang set*, in preparation
- [5] T. K. Springer, F. Veldkamp, *Octonions, Jordan algebras and exceptional groups. Revised English version of the original German notes*. Springer Monographs in Mathematics. Springer: Berlin (2000)